DETAILED ACTION

This Office Action is in response to Applicant's Appeal Brief filed on January 4, 2010.

Claims 1-30 are pending and herein considered.

EXAMINER'S AMENDMENT

An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given in a telephone interview with David Shifren on March 25, 2010.

The application has been amended as follows:

CLAIMS

1. (Currently amended) A method for partitioning of cryptographic functionality so as to permit delegation of at least one of a plurality of distinct portions of the cryptographic functionality from a delegating device to at least one recipient device, the cryptographic functionality being characterized as a graph comprising a plurality of nodes, the method comprising the steps of:

associating a given set of the nodes with a corresponding one of the plurality of distinct portions of the cryptographic functionality; and

transmitting from the delegating device to the recipient device information representative of one or more of the nodes;

the recipient device being configured based on the transmitted information for authorized execution of a corresponding one of the plurality of distinct portions of the cryptographic functionality;

wherein the nodes of the graph are arranged in a plurality of levels with one or more nodes at each level;

wherein the nodes correspond to respective seeds; ~~and~~

wherein a first seed associated with a node of a first one of the levels is computed as a function of a second seed associated with a node of a second one of the levels higher than the first level;

the transmitted information including the first seed but not the second seed;

wherein the delegating device and the recipient device perform distinct functions; and

wherein the delegating device and said at least one recipient device collectively perform the cryptographic functionality.

2. (Original) The method of claim 1 wherein at least one of the nodes of the graph corresponds to a seed the possession of which permits execution of a corresponding one of the distinct portions of the cryptographic functionality.

3. (Original) The method of claim 1 wherein the transmitting step further comprises transmitting from the delegating device to the recipient device information representative of at least two of the nodes.

4. (Original) The method of claim 1 wherein the transmitting step further comprises transmitting from the delegating device to the recipient device information representative of at least one parent node of the graph.

5. (Original) The method of claim 1 wherein the transmitting step further comprises transmitting from the delegating device to the recipient device information representative of at least one child node of a parent node of the graph.

6. (Original) The method of claim 1 wherein the graph comprises at least first and second root nodes.

7. (Original) The method of claim 1 wherein the graph comprises a tree having at least first and second subtrees associated with respective first and second ones of the plurality of distinct portions of the cryptographic functionality.

8. (Original) The method of claim 1 wherein the graph comprises a chain.

9. (Original) The method of claim 1 wherein the graph comprises L levels of nodes, an Lth one of the levels comprising a parent node $v_{L,1}$, and a first one of these levels comprising a set of seeds $v_{1,1}, v_{1,2}, \ldots v_{1,n}$, where n is the total number of seeds, each of the seeds being derivable from the parent node.

10. (Original) The method of claim 9 wherein an ith node of a kth one of the levels is computed as $f_k(i, v_{k+1})$, where f_k is a one-way function.

11. (Original) The method of claim 10 wherein the nodes of one or more of the levels are arranged in the form of tuples of designated numbers of nodes.

12. (Original) The method of claim 11 wherein the ith node of a jth tuple of the kth level is computed as $f_k(j, i, v_{k+1,j})$.

13. (Original) The method of claim 1 wherein the cryptographic functionality comprises a cryptographic functionality provided by a hardware-based authentication token.

14. (Original) The method of claim 1 wherein the cryptographic functionality comprises an ability to verify at least one of an authentication code and a distress code generated by a hardware-based authentication token.

15. (Original) The method of claim 14 wherein the authentication token is configured to store at least two seeds, and the cryptographic functionality comprises a verification operation performed collaboratively by at least first and second servers each storing one of the seeds.

16. (Original) The method of claim 1 wherein the cryptographic functionality comprises an ability to generate at least one of an authentication code and a distress code utilizing a hardware-based authentication token.

17. (Original) The method of claim 1 wherein the cryptographic functionality comprises at least one of an ability to verify a signature and an ability to generate a signature.

18. (Original) The method of claim 1 wherein the cryptographic functionality comprises an ability to generate one or more values of a one-way chain.

19. (Original) The method of claim 1 wherein the cryptographic functionality comprises an ability to perform symmetric cryptographic operations.

20. (Original) The method of claim 1 wherein the cryptographic functionality comprises an ability to perform asymmetric cryptographic operations.

21. (Original) The method of claim 1 wherein the cryptographic functionality comprises an ability to derive one or more cryptographic keys.

22. (Original) The method of claim 1 wherein the cryptographic functionality comprises an ability to compute one or more seeds.

23. (Original) The method of claim 22 wherein at least one of the seeds corresponds to at least one of the nodes of the graph.

24. (Original) The method of claim 1 wherein the cryptographic functionality is partitioned in accordance with a subscription model which requires compliance with at least one specified criterion for transmission from the delegating device to the recipient device of the information representative of one or more of the nodes.

25. (Original) The method of claim 24 wherein compliance with the specified criterion is satisfied upon receipt of a designated payment.

26. (Original) The method of claim 1 wherein the recipient device and the delegating device collaborate to perform at least one of a cryptographic verification function and a cryptographic generation function.

27. (Original) The method of claim 26 wherein the recipient device includes only a limited computational ability associated with performance of the cryptographic function.

28. (Currently amended) An apparatus comprising:

a processing device comprising a processor coupled to a memory;

the processing device being utilized in conjunction with partitioning of cryptographic functionality so as to permit delegation of at least one of a plurality of distinct portions of the cryptographic functionality from the processing device, configured as a delegating device, to at least one recipient device, the cryptographic functionality being characterized as a graph comprising a plurality of nodes;

the processing device being configured to associate a given set of the nodes with a corresponding one of the plurality of distinct portions of the cryptographic functionality, and to transmit to the recipient device information representative of one or more of the nodes, the recipient device being configured based on the transmitted information for authorized execution of a corresponding one of the plurality of distinct portions of the cryptographic functionality;

wherein the nodes of the graph are arranged in a plurality of levels with one or more nodes at each level;

wherein the nodes correspond to respective seeds; ~~and~~

wherein a first seed associated with a node of a first one of the levels is computed as a function of a second seed associated with a node of a second one of the levels higher than the first level;

the transmitted information including the first seed but not the second seed;

wherein the delegating device and the recipient device perform distinct functions; and

wherein the delegating device and said at least one recipient device collectively perform the cryptographic functionality.

29. (Currently amended) An apparatus comprising:

a processing device comprising a processor coupled to a memory;

the processing device being utilized in conjunction with partitioning of cryptographic functionality so as to permit delegation of at least one of a plurality of distinct portions of the cryptographic functionality to the processing device, configured as a recipient device, from at least one delegating device, the cryptographic functionality being characterized as a graph comprising a plurality of nodes;

a given set of the nodes being associated with a corresponding one of the plurality of distinct portions of the cryptographic functionality;

the processing device being operative to receive from the delegating device information representative of one or more of the nodes, the processing device

being configured based on the received information for authorized execution of a corresponding one of the plurality of distinct portions of the cryptographic functionality;

wherein the nodes of the graph are arranged in a plurality of levels with one or more nodes at each level;

wherein the nodes correspond to respective seeds; ~~and~~

wherein a first seed associated with a node of a first one of the levels is computed as a function of a second seed associated with a node of a second one of the levels higher than the first level;

the received information including the first seed but not the second seed;

wherein the recipient device and the delegating device perform distinct functions; and

wherein the recipient device and said at least one delegating device collectively perform the cryptographic functionality.

30. (Currently amended) A non-transitory machine-readable storage medium containing one or more software programs for use in partitioning of cryptographic functionality so as to permit delegation of at least one of a plurality of distinct portions of the cryptographic functionality from a delegating device to at least one recipient device, the cryptographic functionality being characterized as a graph comprising a plurality of nodes, wherein the one or more software programs when executed by the delegating device implement the steps of:

associating a given set of the nodes with a corresponding one of the plurality of distinct portions of the cryptographic functionality; and

transmitting from the delegating device to the recipient device information representative of one or more of the nodes;

the recipient device being configured based on the transmitted information for authorized execution of a corresponding one of the plurality of distinct portions of the cryptographic functionality;

wherein the nodes of the graph are arranged in a plurality of levels with one or more nodes at each level;

wherein the nodes correspond to respective seeds; ~~and~~

wherein a first seed associated with a node of a first one of the levels is computed as a function of a second seed associated with a node of a second one of the levels higher than the first level;

the transmitted information including the first seed but not the second seed;

wherein the delegating device and the recipient device perform distinct functions; and

wherein the delegating device and said at least one recipient device collectively perform the cryptographic functionality.

REASONS FOR ALLOWANCE

Claims 1-30 are allowed.

The following is an examiner's statement of reasons for allowance:

The present invention is directed towards a method, computer program product and apparatus for partitioning of cryptographic functionality so as to permit delegation of at least one of a plurality of distinct portions of the cryptographic functionality from a delegating device to at least one recipient device, the cryptographic functionality being characterized as a graph comprising a plurality of nodes, the method comprising the steps of associating a given set of the nodes with a corresponding one of the plurality of distinct portions of the cryptographic functionality and transmitting from the delegating device to the recipient device information representative of one or more of the nodes, the recipient device being configured based on the transmitted information for

authorized execution of a corresponding one of the plurality of distinct portions of the cryptographic functionality and wherein the nodes of the graph are arranged in a plurality of levels with one or more nodes at each level and wherein the nodes correspond to respective seeds and wherein a first seed associated with a node of a first one of the levels is computed as a function of a second seed associated with a node of a second one of the levels higher than the first level, the transmitted information including the first seed but not the second seed and wherein the delegating device and the recipient device perform distinct functions and wherein the delegating device and said at least one recipient device collectively perform the cryptographic functionality.

Independent claims 1, 28, 29, and 30 each identify the uniquely distinct feature of partitioning cryptographic functionality to permit delegation of at least one of a plurality of distinct portions of cryptographic functionality from a delegating device to at least one recipient device, the cryptographic functionality characterized as a graph comprising a plurality of nodes wherein a given set of nodes is associated with a distinct portion of the cryptographic functionality and wherein the nodes are arranged in a plurality of levels with one or more nodes at each level and wherein the nodes correspond to respective seeds computed as a function of a second seed associated with a node of a higher level and wherein the delegating and recipient devices perform distinct functions and where the delegating and recipient devices collectively perform the cryptographic functionality.

The closest prior art, United States Patent Application Publication No. 2002/0094088 to Takumi Okaue, discloses partitioning cryptographic functionality to

permit delegation of at least one of a plurality of distinct portions of cryptographic functionality from a delegating device to at least one recipient device, the cryptographic functionality characterized as a graph comprising a plurality of nodes wherein a given set of nodes is associated with a distinct portion of the cryptographic functionality and wherein the nodes are arranged in a plurality of levels with one or more nodes at each level and wherein the nodes correspond to respective seeds computed as a function of a second seed associated with a node of a higher level. Nowhere does Okaue disclose wherein the delegating and recipient devices perform distinct functions and where the delegating and recipient devices collectively perform the cryptographic functionality.

The prior art, either singularly or in combination fails to anticipate or render obvious the present invention.

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Tamara Teslovich whose telephone number is (571)272-4241. The examiner can normally be reached on Mon-Fri 8:00-4:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571) 272-3865. The fax phone

number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Tamara Teslovich/
Examiner, Art Unit 2437

/Matthew B Smithers/
Primary Examiner, Art Unit 2437